



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,407	10/24/2003	Paul C. Roberts	MSFT-2817/301134.01	1473

41505 7590 05/29/2008

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)

CIRA CENTRE, 12TH FLOOR

2929 ARCH STREET

PHILADELPHIA, PA 19104-2891

EXAMINER

CHAI, LONGBIT

ART UNIT

PAPER NUMBER

2131

MAIL DATE

DELIVERY MODE

05/29/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/693,407

**Applicant(s)**

ROBERTS ET AL.

**Examiner**

LONGBIT CHAI

**Art Unit**

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 22 February 2008.  
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-4, 6, 7, 9-14, 16-27 and 29-40 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1-4, 6, 7, 9-14, 16-27 and 29-40 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.  
10) ☒ The drawing(s) filed on 24 October 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_.  
5) ☐ Notice of Informal Patent Application  
6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

1. Currently pending claims are 1 – 4, 6, 7, 9 – 14, 16 – 27 and 29 – 40.

### *Response to Arguments*

2. Some of Applicant's arguments with respect to instant claims 1, 14 and 27 regarding encryption / decryption of user input have been fully considered but are moot in view of the new ground(s) of rejection necessitated by Applicant's amendment.
3. The following Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.
4. As per claim 1, 24 and 37, Applicant asserts "Boebert's video RAM is not a source entity in a secured execution environment. Boebert's source entity is the video port, which is not within a secured execution environment. Boebert does not disclose accepting output from a specific source entity within said secured execution environment and not within said second execution environment; and securely transferring said output to an output device" (Remarks: Page 11 / Last sentence). Examiner respectfully disagrees because a secure video RAM, as taught by Boebert, is qualified as a specific source entity for providing the output data within said secured execution environment to meet the claim language since the video RAM is used only in trusted path mode and not in normal mode (Boebert : Column 8 Line 57 – 63 / Line 45 – 50).
5. As per claim 1, Applicant asserts "Griffin does not disclose determining a specific destination entity within said execution environment for said user input" (Remarks: Page 12 / 3<sup>rd</sup> Para). Examiner respectfully disagrees because Griffin teaches "when the process attempts to perform an operation falling within a second set containing the predetermined operations which can affect security of the host operating system, then a guest operating system is provided for

Art Unit: 2131

running the process” (Griffin: Column 4 Line 50 – 53 and Column 5 Line 33 – 36) – i.e. it is based on the determination whether the operation may affect the security of the host operating system to select the intended execution environment – This is also consistent with the specification that indicates: “determining whether the user input is intended for nexus (i.e. a guest operating system)” (SPEC: Page 14 / Para [0048]) and as such Griffin does teach “determining a specific destination entity within said execution environment for said user input”.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1, 14 and 27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 14 and 27 are indefinite because the claim language “the encrypted user input does not contain an explicit indication of an intended execution environment” is considered to be unclear in the context and scope of its meaning about what exactly to constitute “not containing an explicit indication”. Examiner notes according to the disclosure of the specification, the subject matter of inventions indicates: “determining whether the user input is intended for nexus (i.e. a guest operating system)” (SPEC: Page 14 / Para [0048]) – Therefore, Examiner notes the determination is indeed based on the user input on a selection of execution environment with nexus (i.e. a guest operating system) instead of host operating system, which can be considered as one form of explicit indications.

Any other claims not addressed are rejected by virtue of their dependency should also be corrected.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 11 – 13, 24 – 26 and 37 – 40 are rejected under 35 U.S.C. 102(b) as being anticipated by Boebert et al. (U.S. Patent 5,822,435).

As per claim 11, 24 and 37, Boebert teaches a method for providing a secure user interface to a secured execution environment on a system (Boebert : Figure 4) comprising said secured execution environment and an second execution environment (Boebert : Figure 2 / Element 63 & 69 and Column 4 Line 51 – 53), comprising:

accepting output from a specific source entity within said secured execution environment and not within said second execution environment (Boebert : Column 8 Line 45 – 50: (a) a trusted path mode is considered as a secured execution environment (b) the video RAM as the source of the output is qualified as “an output of a specific source entity within said secured execution environment” to meet the claim language because the video RAM is used only in trusted path mode and not in normal mode); and

securely transferring said output to an output device (Boebert : Column 8 Line 57 – 63 and Column 9 Line 53 – 65: (a) in a secure mode, an output is transferred and stored in to a video RAM, which is not used in a normal mode and outputted to a trusted window and (b) display the data on a trusted window, as taught by Boebert, can be considered as securely transferring the output to an output device).

Art Unit: 2131

As per claim 12, 25 and 38, Boebert teaches encrypting said data portion of said output (Boebert : Column 3 Line 26 – 28: data transferred from an output device is encrypted first).

As per claim 13, 26, and 39, Boebert teaches transferring said output to a curtained memory (Boebert : Column 8 Line 57 – 63: a curtained memory is interpreted as a protected memory area. In a secure mode, an output is transferred and stored in to a video RAM, which is not used in a normal mode and outputted to a trusted window).

As per claim 40, Boebert teaches a trusted rendering interface providing rendering said output from said specific source entity (Boebert : Column 8 Line 48 – 63: a trusted video manager and a trusted window for a specific user screen display); and where said secure transfer is a transfer of said rendered output (Boebert : Column 8 Line 57 – 63: a curtained memory is interpreted as a protected memory area. In a secure mode, an output is transferred and stored in to a video RAM, which is not used in a normal mode and outputted to a trusted window).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Art Unit: 2131

8. Claims 1 – 4, 6 – 7, 9, 10, 14, 16 – 23 and 27, 29 – 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Griffin et al. (U.S. Patent 7,159,210), in view of Boebert et al. (U.S. Patent 5,822,435).

As per claim 1, 14 and 27, Griffin teaches a method for providing a secure user interface to a secured execution environment on a system comprising said secured execution environment and an second execution environment (Griffin: Abstract), comprising:

accepting encrypted (see **Boebert below**) user input intended for either said secured execution environment or said second execution environment (Griffin: Figure 2 / Element 211, Column 5 Line 33 – 60, Column 4 Line 50 – 53 and Column 3 Line 8 – 11: (a) either a host operating system or a guest operating system is provided depends on the level of security concerns (b) an application / process is also considered as a user entity because any application must be initially activated by a user) wherein the encrypted user input does not contain an explicit indication of an intended execution environment (Griffin: Column 4 Line 50 – 53 and Column 5 Line 33 – 60: (a) Also see 112-2<sup>nd</sup> rejection (b) it is based on the determination whether the operation may affect the security of the host operating system to select the intended execution environment and as such it is not an explicit indication of an intended execution environment – This is also consistent with the specification that indicates: “determining whether the user input is intended for nexus (i.e. a guest operating system)” (SPEC: Page 14 / Para [0048]));

determining, based on said decrypted user input, whether said decrypted user input is intended for said secured execution environment (Griffin: Column 4 Line 50 – 53 and Column 5 Line 33 – 60: Also see 112-2<sup>nd</sup> rejection);

if said decrypted user input is not intended for said secured execution environment, transferring said decrypted user input to said second execution environment (Griffin: Griffin: Column 5 Line 33 – 60);

if said decrypted user input is intended for said secured execution environment, determining a specific destination entity within said secured execution environment for said decrypted user input, and transferring said decrypted user input to said specific destination entity (Griffin: Column 4 Line 50 – 53 and Column 5 Line 33 – 36) – i.e. it is based on the determination whether the operation may affect the security of the host operating system to select the intended execution environment – This is also consistent with the specification that indicates: “determining whether the user input is intended for nexus (i.e. a guest operating system)” (SPEC: Page 14 / Para [0048]).

However, Griffin does not explicitly disclose (a) the user input is encrypted (b) decrypting said encrypted user input (c) accepting output from a specific source entity within said secured execution environment and not within said second execution environment and (d) securely transferring said output to an output device.

Boebert teaches:

(a) the user input is encrypted and (b) decrypting said encrypted user input (Boebert: Figure 2 / Element 20 & 35, Column 5 Line 44 – 46 / Line 18 – 24 and Column 4 Line 27 – 32: the keyboard manager intercepts keyboard data intended for workstation and the data is then routed to cryptographic entity, where it is encrypted before being passed over auxiliary port to workstation processing unit).

(b) accepting output from a specific source entity within said secured execution environment and not within said second execution environment (Boebert : Column 8 Line 45 – 50: (a) a trusted path mode is considered as a secured execution environment (b) the video



Art Unit: 2131

RAM as the source of the output is qualified as “an output of a specific source entity within said secured execution environment” to meet the claim language because the video RAM is used only in trusted path mode and not in normal mode; and

(c) securely transferring said output to an output device (Boebert : Column 8 Line 57 – 63 and Column 9 Line 53 – 65; (a) in a secure mode, an output is transferred and stored in to a video RAM, which is not used in a normal mode and outputted to a trusted window and (b) display the data on a trusted window, as taught by Boebert, can be considered as securely transferring the output to an output device).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Boebert within the system of Griffin because (a) Griffin teaches performing secured and non-secured computing operation in a compartmented operating environments (Griffin: Abstract), and (b) Boebert teaches ensuring of a secured protection mechanism when data transferred from the input / output devices over a secured and non-secured operation environments (Boebert: Abstract, Column 5 Line 44 – 46 / Line 18 – 24 and Column 8 Line 45 – 50).

As per claim 2, Griffin as modified teaches said step of accepting user input from a user input device comprises decrypting said user input (Boebert : Column 3 Line 26 – 30).

As per claim 3, 16 and 29, Griffin as modified teaches establishing a secure communications channel with said user input (Boebert : Column 3 Line 26 – 30: the user input is encrypted first).

As per claim 4, 17 and 30, Griffin as modified teaches verifying said user input (Boebert : Column 6 Line 26 – 29).

Art Unit: 2131

As per claim 6, 19, Griffin as modified teaches providing window management functionality for managing at least one graphical user interface element owned by said specific destination entity (Boebert : Column 6 Line 53 – 59 and Column 8 Line 57 – 63); and determining that said user input relates to said graphical user interface element (Boebert : Column Column 8 Line 60 – 63 and Figure 6 / Element 82).

As per claim 7, 20 and 33, Griffin as modified teaches interpreting said user input (Griffin: Column 3 Line 10 – 19).

As per claim 9, 22 and 35, Griffin as modified teaches encrypting said data portion of said output (Boebert : Column 3 Line 26 – 28: data transfrerde from an output device is encrypted first).

As per claim 10, 23 and 36, Griffin as modified teaches transferring said output to a curtained memory (Boebert : Column 8 Line 57 – 63: a curtained memory is interpreted as a protected memory area. In a secure mode, an output is transferred and stored in to a video RAM, which is not used in a normal mode and outputted to a trusted window).

As per claim 18 and 31, Griffin as modified teaches if said user input is intended for said secured execution environment, determining a specific destination entity in said secured execution environment for said user input; and transferring said user input to said specific destination entity (Griffin: Column 5 Line 33 – 60).

As per claim 21 and 34, Griffin as modified teaches accepting output from a specific source entity in said secured execution environment (Boebert : Column 8 Line 45 – 50: a trusted

Art Unit: 2131

path mode is considered as a secured execution environment); and securely transferring said output to an output device (Boebert : Column 8 Line 57 – 63: in a secure mode, an output is transferred and stored in to a video RAM, which is not used in a normal mode and outputted to a trusted window).

As per claim 32, Griffin as modified teaches teaches a trusted window manager that provides window management functionality for managing at least one graphical user interface element owned by said specific destination entity (Boebert : Column 6 Line 53 – 59 and Column 8 Line 57 – 63 & Figure 6 / Element 82: a trusted window is owned by a specific destination entity); and where said trusted input manager determines that said user input relates to said graphical user interface element (Boebert : Column 6 Line 26 – 26 / Line 44 – 59 and Column 8 Line 57 – 63 & Figure 6 / Element 82).

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2131

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai Ph.D.

Primary Examiner, Art Unit 2131

5/19/2008